

M³IS

Online-Zugriff auf multimediale Patientendaten mit mobilen Endgeräten am Krankenbett

Michael Gründler⁽¹⁾, Heyo Spekker⁽¹⁾, Oliver Nee⁽¹⁾, Marco Eichelberg⁽¹⁾,
Kay Kronberg⁽²⁾

¹ Kuratorium OFFIS e.V., Escherweg 2, 26121 Oldenburg

² Klinikum Oldenburg gGmbH, Dr.-Eden-Str. 10, 26133 Oldenburg

michael.gruendler@offis.de
heyo.spekker@offis.de
oliver.nee@offis.de
marco.eichelberg@offis.de
kronberg.kay@klinikum-oldenburg.de

Abstract: Die tägliche Visite auf den Stationen eines Krankenhauses ist der zentrale Punkt zur Kommunikation der behandelnden Ärzte untereinander sowie zur Kommunikation zwischen Arzt und Patient. Multimediale diagnostische Daten wie zum Beispiel Filme von Herzkatheter-Untersuchungen in der Kardiologie und Herzchirurgie sind am Patientenbett in der Regel nicht verfügbar. Mit der vom Land Niedersachsen im Rahmen der "Multimedia-Initiative Niedersachsen" geförderten Entwicklung eines mobilen multimedialen medizinischen Informationssystems (M³IS) soll eine Lösung für dieses Problem geschaffen werden, indem mit einem WLAN eine preiswerte und leistungsfähige Netzwerkinfrastruktur zur Verfügung gestellt wird. Über einen Web-Client wird ein einfacher Abruf der relevanten Daten und klinischen Dokumente ermöglicht. Dieser Beitrag beschreibt Erfahrungen beim inzwischen abgeschlossenen Aufbau der WLAN-Infrastruktur inklusive der notwendigen Maßnahmen zur Absicherung des Netzwerks, verfügbare Endgeräte sowie erste Erfahrungen in der Anwendung des Systems.

1 Einleitung

Das von der „Multimedia-Initiative Niedersachsen“ geförderte Projekt M³IS beschäftigt sich mit der Entwicklung eines mobilen multimedialen medizinischen Informationssystems (M³IS) in drei unterschiedlichen Anwendungsszenarien aus dem klinischen Alltag und wird mit Projektpartnern des Gesundheitswesens (Krankenhaus, Rehabilitationszentrum, niedergelassener Bereich) in der täglichen Praxis erprobt.

Innerhalb des ersten Szenarios wird M³IS zur Verbesserung der Kommunikation zwischen unterschiedlichen Abteilungen eines Krankenhauses eingesetzt. Über Standardschnittstellen wie z. B. HL7 und DICOM werden relevante Patientendaten vom M³IS-

Dokumentenserver gesammelt und den Ärzten für ihre tägliche Arbeit ortsunabhängig über einen web-basierten Client zur Verfügung gestellt. Damit entfällt das Einsortieren von ausgedruckten Untersuchungsbefunden in Patientenakten, die telefonische Nachfrage nach relevanten Patientendaten, ggf. unnötige Doppeluntersuchungen wegen fehlender Untersuchungsergebnisse und das Warten auf Dokumente, die vom Krankenhauspersonal zwischen den Abteilungen transportiert werden.

Das zweite Szenario ermöglicht den einweisenden Ärzten und den Hausärzten, über eine verschlüsselte Web-Schnittstelle wichtige Patientendaten abzurufen. Oftmals ist die Laufzeit der ausführlichen Arztbriefe so hoch, dass die für die Anschlussbehandlung der Patienten nach dem Krankenhausaufenthalt erforderlichen Informationen nicht rechtzeitig bei den weiterbehandelnden Ärzten vorliegen. Die Qualität der Arztbriefe entspricht häufig nicht den Erfordernissen und es fehlen in der Regel auch Medien wie z. B. Herzkatheterfilme. M³IS wird durch den schnellen und sicheren Zugriff auf wichtige Patientendaten die Kommunikation zwischen niedergelassenem Bereich und Krankenhaus verbessern.

Im dritten Szenario wird die Visite mit mobilen Endgeräten ermöglicht. Ärzte und Krankenpflegepersonal stellen auf einem Visitewagen die benötigten Dokumente für die Visite am Krankenbett zusammen. Alle Befunde wie z. B. Laborbefunde werden ausgedruckt, falls sie nicht schon auf Papier vorhanden sind, und in die Patientenakte einsortiert. Dieser Medienbruch wird mit M³IS vermieden, indem die Dokumente auf dem Dokumentenserver gesammelt und den Patienten zugeordnet werden. Mit mobilen Endgeräten und einem WLAN sind sie vom Arzt direkt am Patientenbett einsehbar. Insbesondere Dokumente wie Echokardiographie- oder Herzkatheterfilme sind nun über WLAN direkt am Patientenbett verfügbar und können dort mit dem Patienten besprochen werden. Dieser Artikel beschreibt das Vorgehen im Projekt M³IS zum Aufbau eines WLAN unter Berücksichtigung der besonderen Anforderungen für den Betrieb in einem Klinikum.

2 Aufbau des WLAN

Das Klinikum Oldenburg und das Rehabilitationszentrum Oldenburg sind die Pilotanwender im Projekt M³IS. Auf der 28 Betten umfassenden kardiologischen Station des Klinikums wurde ein WLAN für die Visite mit mobilen Endgeräten installiert. Der Grundriss der Station erstreckt sich auf insgesamt drei Flure im zweiten Stockwerk des Klinikums.

Peyman Roshan und Jonathan Leary beschreiben in [PL03] ein Vorgehensmodell für den Aufbau eines WLANs. Auf dieser Grundlage wurden eine Vorgehensweise entwickelt und die Anforderungen für den Betrieb in einem Krankenhaus integriert. Im Folgenden wird das Vorgehen erläutert und die besonderen Anforderungen beschrieben.

Der Betrieb eines WLAN in einem Krankenhaus unterliegt besonderen Anforderungen zur elektromagnetischen Verträglichkeit, die in der Norm DIN EN 60601-1-2 beschrie-

ben werden. Die Auswahl an WLAN-Geräten, die dieser DIN-Norm entsprechen, ist zurzeit noch sehr überschaubar. Die Wahl bzgl. des Access Points fiel auf ein Gerät der AIRONET 1200 Serie von Cisco, dessen Produktfamilie auch WLAN-Karten für verschiedene mobile Geräte beinhaltet. Des Weiteren ist der Access Point (AP) sowohl mit dem 802.11a- als auch mit einem 802.11b/g-Sendermodul ausrüstbar. Mit 802.11x wird vom IEEE (Institute of Electrical and Electronics Engineers) ein 1997 verabschiedeter herstellerunabhängiger Standard für WLANs beschrieben. Um die Sende- und Empfangsleistungen der Access Points zu erhöhen, wurden externe Antennen eingesetzt. Da die APs inmitten eines Gebäudes positioniert werden, sollten die Antennen für den geplanten Einsatz eine Rundstrahlcharakteristik aufweisen, da von einem Access Point so ein größerer Radius abgedeckt wird und dadurch die Anzahl der benötigten AP minimiert wird. Aus diesem Grund wurden die APs mit jeweils zwei externen omnidirektionalen Cushcraft S2403BH-Antennen ausgestattet.

Das Ausmessen der Funkausleuchtung direkt vor Ort verfolgt mehrere Ziele: Neben der Ermittlung des zu verwendenden Funkstandards soll die Anzahl und die Position der benötigten Access Points bestimmt sowie die zur Verfügung stehende Bandbreite ermittelt werden. Ein Grundriss der mit einem WLAN auszustattenden Station verhilft zu einem Überblick der in Frage kommenden Positionen der Access Points. Dabei ist darauf zu achten, dass sich möglichst wenig sichtbare Hindernisse wie z. B. Wände zwischen den möglichen mobilen Positionen und den APs befinden. In Krankenhäusern, insbesondere in älteren Gebäuden, können sich viele sichtbare und unsichtbare Hindernisse wie alte Fahrstuhlschächte, ehemalige Röntgenräume, mit Edelstahl ausgekleidete Küchen usw. befinden, die den Betrieb eines WLAN empfindlich stören. Des Weiteren kann es durch viele Personenbewegungen auf den Gängen der Station oder durch den bewegten Getränkewagen aus Edelstahl zu dynamischen Störungen kommen. Der Test mit einem Access Point mit einem 802.11a-Modul ergab, dass die Sendeleistung nicht ausreicht, um mehrere Wände zu durchdringen. Erst die Ausstattung der APs mit einem Modul für den 802.11b/g-Standard führte zu der erforderlichen Erreichbarkeit des WLANs auf den verschiedenen Patientenzimmern.

Die Erreichbarkeit des AP wird mit den später verwendeten mobilen Endgeräten auf möglichst vielen mobilen Positionen getestet. Der Verbindungsaufbau und die Zeitdauer zweier Downloads unterschiedlicher Größe mit einem, bzw. gleichzeitig mit zwei mobilen Geräten gibt Aufschluss über die Erreichbarkeit und über die zur Verfügung stehende Bandbreite. Die mögliche Position des AP wird solange verändert, bis sich auf allen erforderlichen mobilen Positionen die gewünschte Erreichbarkeit und Bandbreite einstellt. Da der 802.11b/g-Standard den gleichzeitigen Betrieb von 802.11b- und 802.11g-Clients gestattet, müssen mögliche gegenseitige Beeinflussungen bei den Erreichbarkeitstests berücksichtigt werden.

Aus dem Ergebnis der Ausmessung der Funkausleuchtung auf der Station lässt sich die benötigte Anzahl der APs ablesen. Abbildung 1 zeigt einen Grundriss der Station und die ermittelten Positionen der APs. Die Kreise geben die Reichweite und die Überlappung der einzelnen APs an. Die kardiologische Station bei dem Pilotanwender konnte mit drei Access Points komplett ausgeleuchtet werden. Da auch in Krankenhäusern die Diebstahlsrate sehr hoch ist, müssen geeignete Methoden zur Vermeidung von Diebstählen

angewendet werden. In neueren Krankenhäusern werden die Decken oftmals mit einem für Funkwellen leicht durchdringbaren Material wie Gips oder Karton verkleidet. Hier bietet sich die Möglichkeit, die APs inklusive der Antennen unsichtbar für das Auge zu installieren. Sollte das Deckenmaterial aus nicht oder nur schwer durchdringbarem Material wie z. B. Blech bestehen, müssen zumindest die Antennen sichtbar installiert werden. Der von der DIN VDE 0848-2 [DIN] und der 26. Verordnung zum Bundes-Immissionsschutzgesetz [BISG] festgelegte Mindestabstand von WLAN-Antennen zu Personen von 50 cm ist unbedingt einzuhalten. Des Weiteren ist darauf zu achten, dass Antennen inklusive der Befestigung nicht in die Durchgangsbereiche hineinragen.

Access Points benötigen sowohl einen Zugang zum Netzwerk des Klinikums als auch eine Stromversorgung. Durch den Einsatz von „Power over Ethernet“ (PoE) wird der Installationsaufwand verringert und die Flexibilität erhöht. Dabei wird auf noch unbenutzten Adern des ohnehin anzuschließenden Netzkabels die benötigte Versorgungsspannung der AP gelegt. Bei der Beschaffung ist unbedingt auf die Kompatibilität der Geräte zu achten. Manche Hersteller halten sich nicht an den „Power over Ethernet“ Standard der Spezifikationen IEEE 802.3af und sind nicht kompatibel mit anderen Herstellern.

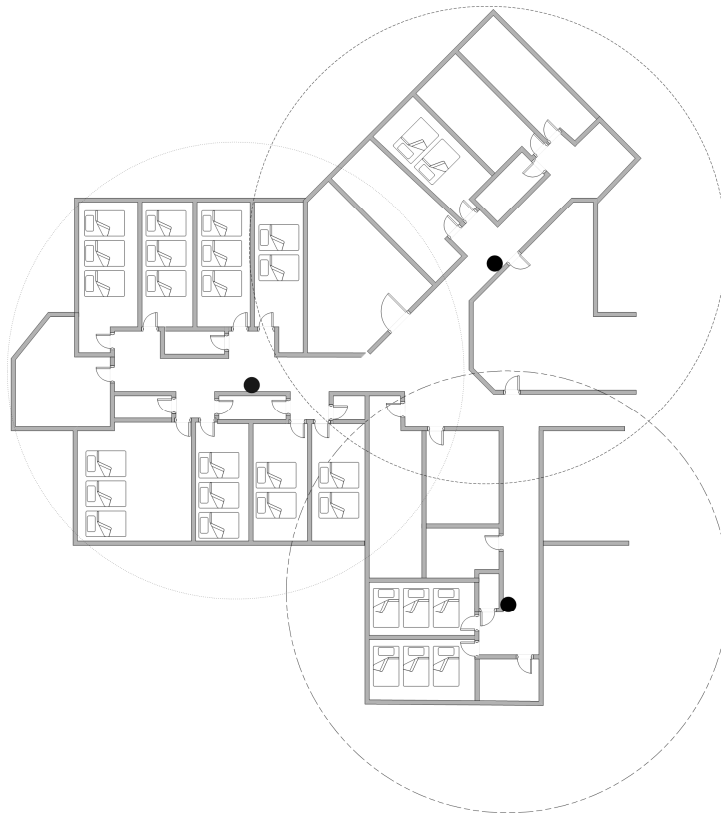


Abbildung 1: Position der AP auf der Station und deren Reichweite

Nachdem die APs an den zuvor ermittelten Positionen befestigt wurden, muss die Wiederholung des Funkausleuchtungstests das gewünschte Ergebnis bestätigen. Dabei wird unter anderem überprüft, ob auch das automatische Umschalten der WLAN-Clients auf den jeweils stärksten AP (Roaming) den Erfordernissen entspricht. Die APs wurden auf die im 2,4 GHz Frequenzband des 802.11g-Standard zur Verfügung stehenden drei überlappungsfreien Kanäle verteilt. Somit ist sichergestellt, dass es auch in Gebieten, in denen sich die Ausleuchtung von mehreren Access Points überschneidet zu keinen gegenseitigen Störungen der APs kommen kann.

3 Sicherheitskonzept

Da im Krankenhausnetzwerk überwiegend personenbezogene Daten übertragen werden, müssen besondere Schutzmechanismen gegenüber Mithören und Manipulation der Daten eingesetzt werden. Insbesondere ein drahtloses Netzwerk ist einem erhöhten Risiko ausgesetzt, da es aufgrund der funkbasierten Datenübertragung eine größere Angriffsfläche bietet. Das WLAN endet nicht an den Gebäudegrenzen, und potentielle Angreifer können aufgrund von ungewollten Reichweiten der AP auch versteckt von außen Angriffsversuche starten. Deutlich leichter als in drahtgebundenen Netzwerken kann ein Angreifer den Netzwerkverkehr mitschneiden und ihn analysieren, um dann basierend auf den gewonnen Zugangsdaten auf das WLAN zugreifen zu können. Da dieser Ansatz passiv ist, ist er nur schwer zu entdecken. Aus diesem Grund müssen nicht nur die übertragenen Daten geschützt, sondern auch der Zugang zum WLAN kontrolliert werden. Die Verwendung unterschiedlicher Client-Geräteklassen im Projekt M³IS erfordert außerdem einen kompatiblen Einsatz von kryptographischen Methoden. Obwohl die gesamte Hardware des WLANs von einem Hersteller stammt, erfüllen nicht alle Betriebssysteme bzw. die mobilen Endgeräte die gleichen Voraussetzungen. Insgesamt umfasst das WLAN-Sicherheitskonzept die folgenden Sicherheitsmaßnahmen:

- *MAC- und IP-Filter:* WLAN-Karten sind ebenso wie Netzwerkkarten mit einer weltweit eindeutigen MAC-Adresse (Media Access Control Address) ausgestattet. Das Filtern von MAC- und IP-Adressen der Clients auf dem Access Point zur Zugangskontrolle bietet nur einen geringen Schutz, da diese auch mit nur geringem Fachwissen gefälscht werden können, stellt aber eine erste Hürde dar, die ein Angreifer überwinden muss. Ab Windows 2000 ist die softwareseitige Änderung der MAC Adresse mit dem Programm [SMAC] möglich.
- *WEP und WPA:* Der weit verbreitete Verschlüsselungsstandard WEP (Wired Equivalent Privacy) [R04a] hat hinlänglich bekannte Angriffspunkte [HRB03], stellt aber ebenfalls eine Hürde für einen potentiellen Angreifer dar. Borisov et. al. beschreiben in [BGW01] ausführlich unterschiedliche Angriffsmöglichkeiten gegen WEP. Im Kontext der in M³IS verwendeten mobilen Endgeräte ist WEP mit statischen Schlüsseln und 128-Bit-Verschlüsselung Vorbedingung für die Nutzung von TKIP (s.u.). WPA (Wi-Fi Protected Access), der Nachfolger von WEP, konnte bis-

lang nicht verwendet werden, da nicht alle anzubindenden mobilen Clients über ausreichende Treiberunterstützung verfügen.

- *TKIP*: Die Verwendung von TKIP (Temporary Key Integrity Protocol) [R04b] mit kurzer Periodendauer der Rotation der temporären Schlüssel bietet mehr Sicherheit. Eine Integritätskontrolle mit der Bezeichnung MIC (Message Integrity Check) ist Bestandteil von TKIP. MIC ist wesentlich komplexer als der im WEP implementierte ICV (Integrity Check Value) und verhindert unerkannte Datenmanipulationen und ein systematisches Vertauschen von Bits in verschlüsselten Frames (Bit Flipping). Des Weiteren wird die so genannte Replay-Attacke verhindert, indem über eine Sequenznummer überprüft wird, ob ein Datenpaket bereits gesendet wurde.
- *Paketfilter*: Über den Paketfilter des AIRONET 1200 lassen sich alle nicht benötigten Protokolle bzw. Ports abschalten. Mit dieser Zugriffskontrolle kann sichergestellt werden, dass wirklich nur die Dienste des Netzwerks verwendet werden, die im Projekt M³IS unbedingt erforderlich sind.
- *RADIUS*: Mit Hilfe von RADIUS (Remote Authentication Dial-in User Service) [RFCa] kann eine benutzerbezogene Zugangsbeschränkung realisiert werden, über die genau festgelegt werden kann, welcher Benutzer auf welche Ressourcen Zugriff hat. Die geplante Installation eines RADIUS-Servers mit einer sicheren Benutzerauthentifikation über Zertifikate bietet Sicherheit im WLAN nach aktuellen Standards.
- *SSL/TLS*: Über die Verbindung zwischen WLAN-Client und Access Point hinweg wird die Kommunikation zwischen dem M³IS-Server und den verschiedenen Clients durch das Transport Layer Security-Protokoll (TLS) bzw. durch dessen Vorgänger (Version 3 der Secure Sockets Layer, SSL) [RFCb] abgesichert. Durch diese Maßnahme werden Integrität und Vertraulichkeit der Datenübermittlungen sichergestellt.

Zusätzlich zu den gewählten Sicherheitsmechanismen gibt es eine Vielzahl von Konfigurationsmöglichkeiten auf dem AP. Das Verändern aller sicherheitsrelevanten Standardeinstellungen wie z. B. die (E)SSID (Extended Service Set Identifier), der Access Point-Administratorname, das Administrator-Passwort und die Administration des AP über SSL ist eine notwendige aber nicht hinreichende Voraussetzung für die Sicherheit im WLAN. Erst die Kombination der vorgestellten Sicherheitsmaßnahmen führen zu einem Mindestmaß an Sicherheit.

4 Endgeräte



Abbildung 2: Mobile Endgeräte: Convertible, Slate und Skeye.pad

Dem Projekt M³IS stehen die in Abbildung 2 dargestellten Typen von mobilen Endgeräten für die Visite im Klinikum zur Verfügung. Allen verwendeten mobilen Geräten ist die Stiftbedienung gemeinsam:

- *Convertible:* Die verwendeten Tablett-PCs der Bauform „Convertible“ mit Tastatur und schwenkbarem Display haben eine Auflösung von 1024×768 , 32 Bit Farbtiefe und 256 echte Graustufen. Das Gerät ist ausgerüstet mit einem Intel Pentium M Prozessor mit 1400 MHz und 512 MB RAM, wiegt ca. 1,9 kg und hat eine Akkulaufzeit von ca. 3 Stunden. Die Geräte sind ausgestattet mit einer CISCO AIR 802.11a/b/g Karte. Als Betriebssystem dient die Windows XP Tablet PC Edition 2005 von Microsoft.
- *Slate:* Die Tablett-PCs der Bauform „Slate“ haben keine Tastatur. Sie verfügen ebenso wie die Convertibles über eine Auflösung von 1024×768 mit 32 Bit Farbtiefe und 256 echten Graustufen. Die Geräte sind mit einem Intel Pentium M Prozessor mit 1000 MHz und 512 MB RAM ausgerüstet, wiegen ca. 1,5 kg und haben eine Akkulaufzeit von 3,5 bis 4 Stunden. Die Geräte verfügen über eine CISCO AIR 802.11a/b/g Karte. Als Betriebssystem dient die Windows XP Tablet PC Edition 2005 von Microsoft.

- *Skeye.pad*: Die Webpads des Projektpartners Höft & Wessel Skeye Webpanel haben keine Tastatur, aber ein Touch-Screen mit einer Auflösung von 800 × 600, 65.536 Farben und 64 Graustufen. Als Prozessor kommt eine Strong ARM CPU mit 206 MHz und 64 MB RAM zum Einsatz. Die Geräte sind über die PCMCIA-Schnittstelle mit einer CISCO AIRONET 350 WLAN-Karte ausgestattet. Das Gewicht wird mit ca. 0,9 kg angegeben, die Akkulaufzeit mit ca. 5 Stunden. Als Betriebssystem dient Microsoft Windows CE .NET 4.2.

Die Tablett-PCs zeichnen sich durch die starke Rechenleistung, den Farbraum des Displays und die flexible WLAN-Anbindung aus. Nachteilig sind der hohe Preis, das hohe Gewicht und die geringe Akkulaufzeit. Die Stärken der Webpads sind die niedrigeren Anschaffungskosten, geringes Gewicht und lange Akkulaufzeiten. Nachteilig ist hier die geringe Auflösung des Displays, der kleine Farbraum, eine vergleichsweise geringe Rechenleistung und knapp bemessener Speicher. Im Gegensatz zu den Tablett-PCs ist die WLAN-Anbindung derzeit nur mit 11 MBit möglich. Die Darstellung von Dokumenten im HTML-, PDF-, Word- und ASCII-Format ist auf allen mobilen Geräten möglich. Das Abspielen von Herzkatheter- und Echokardiographiefilmen ist auf den Webpads nur eingeschränkt möglich. Für das Anzeigen von DICOM-Objekten existieren für das Betriebssystem der Webpads zurzeit keine Viewer. Des Weiteren sind die zur Verfügung stehende Rechenleistung und Speicher der Webpads für die Darstellung von größeren DICOM-Objekten nicht ausreichend. Ist auf einem Endgerät kein DICOM-Viewer installiert oder verfügbar, so kann der M³IS-Server DICOM-Objekte in JPEG-Bilder bzw. MPEG-Filme konvertieren, die ohne zusätzlich zu installierende Software angezeigt werden können. Dabei gehen die Funktionen verloren, die ein DICOM-Viewer anbietet, etwa das Fenster und Ausmessen von Bildern. Tabelle 1 zeigt eine Gegenüberstellung der wichtigsten Parameter der mobilen Endgeräte.

Bauform	Convertible	Slate	Skeye.pad
Prozessor, MHz	Pentium M, 1400	Pentium M, 1000	Strong ARM, 206
Hauptspeicher	512 MB	512 MB	64 MB
Farben	32 Bit	32 Bit	16 Bit
Graustufen	256	256	64
Touch-Screen	nein	nein	ja
Gewicht (gg)	1,4	1,5	0,9
Akkulaufzeit (h)	3	3-4	5
WLAN	802.11a/b/g	802.11a/b/g	802.11b
MPEG abspielen	ja	ja	eingeschränkt
DICOM-Objekte darstellen	ja	ja	nein
Preis ca. (€)	1900	1600	1000

Tabelle 1: Vergleich der mobilen Endgeräte

5 Zusammenfassung

Im Klinikum Oldenburg wurde auf einer kardiologischen Station für die Visite mit mobilen Endgeräten ein Zugriff auf einen M³IS-Server über ein WLAN errichtet. Die Station wird mit insgesamt drei Access Points, die den elektromagnetischen Anforderungen für den Krankenhausbetrieb entsprechen, komplett ausgeleuchtet. Mit unterschiedlichen Sicherheitsmaßnahmen wie z. B. mit WEP und TKIP kryptografisch verschlüsselte Verbindungen und Serverzugriff über SSL/TLS-Verbindungen wird das WLAN gegen unbefugte Benutzung sowie Abhören und Manipulation von Daten geschützt. Unterschiedliche mobile Endgeräte werden für die mobile Visite eingesetzt und werden weiterhin auf ihre Eignung hin untersucht. Über einen Web-Browser wird den Ärzten der Zugang zum M³IS-Server ermöglicht. Nachdem sie sich auf dem M³IS-Server mit Benutzername und Passwort authentifiziert und angemeldet haben, stehen ihnen für alle Patienten ihrer Stationen unterschiedliche Informationen zur Verfügung. Zu den Informationen bzw. Dokumenten gehören: Stammdaten der Patienten, Untersuchungs-Befunde im PDF-, ASCII-, HTML-Format, eingescannte Dokumente im TIFF-Format, Herzkatheter- und Echokardiographie-Bilder im JPEG-Format, Herzkatheter- und Echokardiographie-Filme im AVI-Format und DICOM-Objekte im DICOM-Format. Insgesamt konnte mit dem WLAN eine kostengünstige, kryptografisch gesicherte und mobile Anbindung einer kardiologischen Station an einen Dokumentenserver geschaffen werden. Die Erfahrungen aus der Installation fließen direkt in die WLAN-Anbindung weiterer Stationen ein.

Literaturverzeichnis

- [BGW01] Nikita Borisov, Ian Goldberg, David Wagner: Intercepting Mobile Communications: The Insecurity of 802.11. In: Proceedings of the 7th annual international conference on Mobile computing and networking. Rom 2001, S. 180-189
- [BISG] Verordnung über elektromagnetische Felder, Sechszwanzigste Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (26. BimSchV), BGBI. I 1996; S. 1.966
- [DIN] DIN VDE 0848-2, Sicherheit in elektromagnetischen Feldern; Schutz von Personen im Frequenzbereich von 30 kHz bis 300 GHz , 1991
- [HRB03] M. Tran-Huu, J. Ranke, H. Bludau: WLAN im Gesundheitswesen Sicherheitslücken und rechtliche Implikationen. In: Mobiles Computing in der Medizin - 3. Workshop der Projektgruppe Mobiles Computing in der Medizin (MoCoMed). Köllen Druck + Verlag GmbH, 2003; S. 135 – 143
- [PL03] Peyman Roshan, Jonathan Leary: 802.11 Wireless LAN Fundamentals, 2003, Cisco Press.
- [RFCa] RFC 2138: Remote Authentication Dial In User Service (RADIUS), 1997, <http://www.ietf.org/rfc/rfc2138.txt>, letzter Zugriff: 22.06.2005
- [RFCb] RFC 2246: The TLS Protocol Version 1.0; 1999, <http://www.ietf.org/rfc/rfc2246.txt>, letzter Zugriff 30.06.2005
- [R04a] Jörg Rech: Wireless LANs 802.11-WLAN-Technologie und praktische Umsetzung im Detail, 2004, Heise Zeitschriften Verlag, S. 212-217
- [R04b] Jörg Rech: Wireless LANs 802.11-WLAN-Technologie und praktische Umsetzung im Detail, 2004, Heise Zeitschriften Verlag, S. 377- 378
- [SMAC] SMAC, <http://www.klccconsulting.net/smac/>, Letzter Zugriff 30.06.2005